



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/569,961

02/28/2006

Masao Nonaka

2006_0225A

3341

513

7590

09/29/2009

WENDEROTH, LIND & PONACK, L.L.P.

1030 15th Street, N.W.,

Suite 400 East

Washington, DC 20005-1503

EXAMINER

BAYOU, YONAS A

ART UNIT

PAPER NUMBER

2434

MAIL DATE

DELIVERY MODE

09/29/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/569,961	Applicant(s) NONAKA ET AL.	
	Examiner YONAS BAYOU	Art Unit 2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 February 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☐ Claim(s) _____ is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☒ Claim(s) 1-36 are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 February 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>02/28/2006, 04/25/2006 and 05/11/2006</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Election/Restrictions

1. This application contains claims directed to the following patentably distinct species:

Group 1: Figures 1-6, 8-26, 28-45, and 46-53 associates with claims 1-17, and 26-36.

Group 2: Figures 7, 27, and 46 associates with claims 18-25.

2. The groups are independent or distinct because each of the various disclosed species details a mutual exclusive characteristics of:

Group 1. A key distribution system for distributing shared keys, said key distribution system comprising:

a server which generates common information based on each of the shared keys and distributes the common information; and

receiving devices each of which obtains the shared key based on the common information and an individual intermediate key group set,

wherein each of said receiving devices has been previously provided with at least one individual intermediate key group set which has been selected from among individual intermediate key group sets including at least two different types of individual intermediate key group sets, each of the individual intermediate key group sets including individual intermediate key groups, and

Art Unit: 2434

each of the individual intermediate key groups being made up of one or more individual intermediate keys which have been generated based on one or more system secret variable groups,

said server and said receiving devices can communicate via a communication channel,

said server includes: a shared key storage unit operable to store the shared keys; a system secret variable group storage unit operable to store the system secret variable group sets which are made up of the previously provided system secret variable groups;

each of common information generation units operable to generate the common information based on each shared key;

a common information generation unit selection unit operable to select one of said common information generation units; and

a common information distribution unit operable to distribute the common information to said receiving devices simultaneously or at different times,

each of said common information generation units is operable to generate key update data based on the system secret variable group set and the shared key and operable to generate, using a different common information generation method, common information including (a) a common information identifier and (b) the key update data, the common information identifier

corresponding to the common information generation method, each of said receiving devices includes:

Art Unit: 2434

a common information receiving unit operable to receive the common information;

an individual intermediate key group storage unit operable to store the individual intermediate key group sets each of which is made up of the individual intermediate key groups corresponding to each of the common information generation methods;

shared key obtainment units which respectively correspond to said common information generation units; and

a shared key obtainment unit selection unit operable to select one of said shared key obtainment units,

said shared key obtainment unit selection unit is operable to select one of said shared key obtainment units based on the common information identifier included in the common information which has been received by said common information receiving unit, and

each of said shared key obtainment units is operable to obtain the shared key, using the common information, based on the shared key obtainment method corresponding to the common information identifier and the individual intermediate key group; and

Group 2. A receiving device in a key distribution system comprising a server which distributes shared keys and receiving devices which receive the shared keys, said receiving device comprising:

Art Unit: 2434

a common information receiving unit operable to receive the common information from outside;

an individual intermediate key group storage unit operable to store individual intermediate key group sets each of which is made up of individual intermediate key groups corresponding to each of the common information generation methods;

shared key obtainment units which correspond to said common information generation methods; and

a shared key obtainment unit selection unit operable to select one of the shared key obtainment units,

wherein said shared key obtainment unit selection unit is operable to select the shared key obtainment unit based on the common information identifier included in the common information which has been received by said common information receiving unit, and

said shared key obtainment unit is operable to obtain the shared key, using the common information, based on the shared key obtainment method corresponding to the common information identifier and the individual intermediate key group.

3. Applicant is required under 35 U.S.C. 121 to elect a single disclosed groups for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable. Currently, no claims are generic.

Art Unit: 2434

Applicant is advised that a reply to this requirement must include an identification of the groups that is elected consonant with this requirement, and a listing of all claims readable thereon, including any claims subsequently added. An argument that a claim is allowable or that all claims are generic is considered nonresponsive unless accompanied by an election.

Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional groups which depend from or otherwise require all the limitations of an allowable generic claim as provided by 37 CFR 1.141. If claims are added after the election, applicant must indicate which are readable upon the elected groups. MPEP § 809.02(a).

4. Applicant is advised that the reply to this requirement to be complete must include (i) an election of a group of invention to be examined even though the requirement be traversed (37 CFR 1.143) and (ii) identification of the claims encompassing the elected invention.

The election of an invention or groups may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse.

Should applicant traverse on the ground that the inventions or groups are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions or groups to be obvious variants

Art Unit: 2434

or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C.103 (a) of the other invention.

5. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2434

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yonas Bayou/

Examiner, Art Unit 2434

09/24/2009

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434